**ABSTRACT OF THE DISCLOSURE**

This invention intends to reduce the amount of calculation required by a cipher strength estimating device for estimating a ciphertext in collectively finding session keys for plural rounds of transformation. The cipher strength estimating device is configured to: first calculate one session key prospect presumed to be equivalent to a session key for use at a certain round of transformation in encryption which is calculated from a key; perform a decrypting operation with the session key prospect presumed to be true; calculating a session key prospect for the round immediately preceding the certain round based on the resulting text thereby calculating session keys for different rounds. This device enhances the possibility that plural true session keys are calculated faster.

Fig. 1

1...CONTROL UNIT, 2...PUTATIVE TRANSFORMED TEXT, 3...PUTATIVE UNTRANSFORMED TEXT CALCULATING UNIT, 4...RECALCULATION REQUEST DATA, 5...PLAINTEXT, 6...PUTATIVE UNTRANSFORMED TEXT CALCULATING UNIT, 7...SESSION KEY PROSPECT, 8...SESSION KEY PROSPECT CALCULATING SECTION, 9...UNCALCULABILITY IDENTIFIER DATA, 10...PUTATIVE UNTRANSFORMED TEXT

Fig. 2

1...CIPHERTEXT OR PUTATIVE UNTRANSFORMED TEXT, 2...FIRST PUTATIVE UNTRANSFORMED TEXT CALCULATING SECTION, 3...PUTATIVE UNTRANSFORMED TEXT CALCULATING UNIT BODY, 4...FIRST SESSION KEY PROSPECT CALCULATING SECTION

Fig. 3

101...CPU, 102...INTERNAL MEMORY, 103...EXTERNAL STORAGE UNIT, 104...COMMUNICATION INTERFACE, 105...DISPLAY, 106...INPUT MEANS,

Fig. 4

3...PLAINTEXT AND CIPHERTEXT CALCULATING UNIT